Russian President Vladimir Putin and General Valery Gerasimov observe actions of troops of Russia and Belarus at main stage of Zapad 2017 joint strategic exercises at Luzhsky training ground in Leningrad Region, September 2017 (President of Russia)

When Dragons Watch Bears
Information Warfare Trends and Implications for the Joint Force

By Christopher H. Chin, Nicholas P. Schaeffer, Christopher J. Parker, and Joseph O. Janke

> *The predominance of the psychological over the physical, and its greater constancy, point to the conclusion that the foundation of any theory of war should be as broad as possible.*
>
> —B.H. Liddell Hart, *Strategy*[1]

Lieutenant Colonel Christopher H. Chin, USAF, is Branch Chief in the Future Operations Division at U.S. Cyber Command. Lieutenant Colonel Nicholas P. Schaeffer, USAF, is Chief of Intelligence aboard the National Airborne Operations Center at U.S. Strategic Command. Major Christopher J. Parker, USA, is a Strategic Planner for the Joint Staff J7 at Fort Leavenworth, Kansas. Major Joseph O. Janke, USA, is the Plans and Exercises Chief for the Eighth Army G9 in Camp Humphreys, Korea.

Over the past decade, the People's Republic of China (PRC) has watched Russia's employment of information warfare (IW) with great interest. With the recent conflict in Ukraine and the 2014 Russian annexation of Crimea, the PRC is actively gauging Western nations' response and associated global implications should it choose to forcefully reunify Taiwan. As the current pacing threat, the PRC seeks to rewrite global norms with the intent to assert supreme influence over Taiwan and the Asia-Pacific region. The parallels between these two Great Powers and their associated aggression toward breakaway republics present an opportunity for the United States and the joint force to map the contours of an evolving Chinese information warfare strategy to build a more comprehensive U.S. response prior to a

Marine Corps Sergeant Estefany Gomez Prado, psychological operations specialist with Psychological Operations Company, I Marine Expeditionary Force Information Group, talks to role player during Marine Air Ground Task Force Warfighting exercise 3-22 at Marine Corps Air Ground Combat Center Twentynine Palms, California, May 1, 2022 (U.S. Marine Corps/Benjamin Aulick)

future conflict in the region. Given the scope, sophistication, and scale of modern information warfare activities, thwarting Chinese information confrontation tactics during crisis and conflict will require a comprehensive approach, one that boldly marshals increased unity of effort from across the whole of government. To compete and win in the 21st-century information environment, the Department of Defense (DOD), in partnership with the interagency community, should endeavor to lead three initiatives across upcoming joint force time horizons:

- increase the scope and scale of irregular and information warfare to better fit within the modern competition continuum below the threshold of armed conflict (next 1 to 3 years)
- advocate to establish a central organization responsible for synchronizing U.S. whole-of-government information-related activities to counter foreign malign influence (next 3 to 5 years)
- revive service to the Nation in the digital age with the establishment of a Civilian Cyber Corps as a precursor to a seventh military branch, U.S. Cyber Force, to build the force capacity necessary to execute cyber effects operations at a scale necessary to defend the Nation, its networks, and its traditional military operations (next 5 to 7 years).

Chinese Reflections on Russian IW Activities

Much like their Chinese counterparts, Russian leaders today believe that Western democratic economic prosperity has come at their expense. The concept of *maskirovka*, or military deception, is not simply a strategic approach to conflict—rather, it is a Russian whole-of-government approach to control international perception of Russian activities to set the conditions necessary to achieve national interests.[2] Central to the concept of maskirovka are IW activities designed to distract, overload, paralyze, exhaust, deceive, divide, pacify, deter, provoke, overload, and pressure an adversary.[3] These tactics can be employed individually; however, what is compelling is the seamless orchestration of Russian IW activities with military maneuvers designed to seize the initiative, secure the element of surprise, obfuscate malicious intent, and ultimately deflect Russian attribution, thus delaying strategic consequences until it is too late for organized international response.[4] Among the most prevalent means by which maskirovka has been executed are false flag operations, employment of proxies to engage in disinformation activities, use of private military/mercenary firms such as the Wagner Group, and employment of third-party hacktivists to obfuscate direct attribution to the Russian government across parts of Eastern Europe, Africa, the Middle East, and the United States. These efforts are often used in concert to prepare the environment prior to exercise or conflict.

Four major Russian exercises, which rotate between their military districts (Zapad [west], Vostok [east], Tsentr [center], and Kavkaz [Caucasus, in the Russian southern military district]), became an annual affair following the 2008 Russian army invasion of Georgia. These exercises grant Moscow flexibility to conceal its intentions and while conditioning the operational environment, enabling them to exceed the 13,000-troop limit requiring foreign observers under the Vienna Document.[5] In almost every instance, IW activities preceded major Russian military exercises, usually playing to a "besieged castle" mentality prevalent among Russian policymakers. Russian information activities prior to Zapad 2014 (and the Russian annexation of Crimea) focused on a strategic narrative meant to cause fearful discourse—the exercise scenario depicted terrorism backed by North Atlantic Treaty Organization members Poland and Lithuania against the Russian territories of Belarus and Kaliningrad Oblast.[6] This offered the Russians two predominant benefits in their annexation of Crimea: the ability to cast their intentions as defensive in nature based on a fictional exercise scenario and to motivate its populace into supporting a presupposed cause and effect of defending ethnic Russians in Crimea.

By comparison, China has not engaged in IW activities prior to a strategic military exercise at scale comparable to those of its northern neighbor. There is similarity in the "besieged castle" mindset, where China has crafted the threat of terrorism among its Uighur population,[7] and the creation of laws in Hong Kong making "secession, subversion of the central government, terrorism, or collusion with foreign forces punishable by up to life in prison."[8] China has used this narrative to great effect and is now poised to learn even more from Russia, recently hosting Russian troops for joint strategic drills inside the PRC for the first time.[9]

As authoritarian governments, both China and Russia have successfully demonstrated a willingness and ability to coordinate IW activities across their whole of government. These regimes have the mechanisms to execute a deliberate information campaign to achieve ends that conflict with international norms and expectations for responsible conduct by civilizations in the 21st century. The United States is disadvantaged in this realm and should be concerned that Russia and China are taking steps to learn more from each other to counter Western influence in their respective spheres of influence.

Chinese IW Lessons Learned

Chinese propagandists have studied Russian techniques of flooding the information space with false narratives and wish to emulate Russian success in influencing U.S. actions and sentiment. A concept in Chinese political discourse called *huayu chizi* references a deep-seated feeling that China is maligned or, worse, ignored during global discussion and debate.[10] The remedy to this is strengthening its own *wai xuan*, or external messaging (propaganda) to spread the PRC message in a positive light. To execute this plan, Chinese media leadership described the use of media outlets such as Russia Today (RT) as an "external propaganda aircraft carrier" that should be used to affect social media and break through foreign media environments.[11] A 2018 *People's Daily* article noted favorably that RT had a sizable and growing presence on Facebook, Twitter, and YouTube, as well as a vast growing network of media partnerships across the globe. Furthermore, Russian media strategy was summarized as being a two-part unified strategy: one, presenting a positive expression of Russian views and perspectives on world events, and two, displaying Russian culture and the nation in a positive light. Although the Chinese analysts noted that *wai xuan* would not be the decisive factor in altering sentiment in the West, it would counter negative narratives and add dissonance to anti-Chinese media narratives.[12]

There is also a growing overt acknowledgment that Russian lessons learned are worth studying by Chinese propagandists. Russia and China have held an annual "Internet Media Cloud Forum" since 2015. The most recent iteration occurred in late 2020 and featured keynote speeches by the editor in chief of *China Daily* and the Russian deputy minister of digital development, communications, and mass media. This gathering was focused on increasing Chinese-Russian communication via new information technologies such as artificial intelligence, so-called big data, and 5G telecommunication systems. In addition, Russian and Chinese leaders pledged to build media cooperation by creating "media innovation research centers" and "talent exchange" products—processes widely understood to create a pathway for Russian information techniques to filter into Chinese operations.[13] Although cooperation is still limited, the connection has been established. While it is likely that Russian actions could not be copied perfectly by Chinese IW specialists, there are undeniable signs of learning and adopting Russian techniques, particularly RT's success in presenting and amplifying "alternative" views to Western audiences.

This position is also being advocated in publicly available Chinese research journals. Writing admiringly about Russian information operations targeted to the West, one author explains how "external communication power" is an important part of the country's soft power. In recent years, China has also

Chinese President Xi Jinping boards aircraft carrier *Shandong* and reviews guards of honor at naval port in Sanya, Hainan Province, December 17, 2019 (Xinhua/Li Gang

Ukrainian President Volodymyr Zelensky autographs Ukrainian flag for frontline troops during visit to defensive lines, December 20, 2022, in Bakhmut, Donetsk Oblast, Ukraine (Ukrainian Presidential Press Office)

been continuously strengthening its external communication capabilities to model RT's success in penetrating the Western mind. Russia's national system and information processes have created an increasingly complete and unique international communication system.[14] In late 2015 the Sputnik Chinese News Service was officially launched; it successively opened Weibo and WeChat public accounts to increase official and unofficial cooperation between Russian and Chinese state-run media. In 2015, RT also signed a cooperation agreement with the China News Agency to carry out long-term cooperation on joint interviews and news events.

More concerning is the growing Chinese military boldness in the South China Sea and other areas, spurred by Beijing's perception of being in a "period of strategic opportunity."[15] The PRC is implementing an approach that is uncannily Russian in growing its reach and strategic positioning through actions below the threshold of activating the international community against China or provoking the United States into military conflict.

There are specific ways in which the Chinese media environment observed Russian actions in Crimea and absorbed associated lessons. First, during the preparation period for the war of public opinion, RT described the agenda in economic terms and avoided political terms to prevent comparisons to European and American Cold War attitudes. This presages Chinese activity in the South China Sea—China is only "securing trade routes" and "ensuring Chinese economic zones are respected." Second, during the rising period of conflict, Russian media shifted the topic from economic to political, describing anti-Russian protesters as rioters and terrorists and invoking a dual dilemma of political crisis and economic crisis. This connecting of political ends via economic justification is also very clear in Chinese justification of territorial growth in international waters. Third, Russia continued to use historical and democratic arguments to reduce international willingness to intervene, citing arguments such as "This is what the people want" and "This land has always belonged to Russia," which Chinese propagandists are actively using to justify a huge range of military and economic encroachments along its southern shores. These arguments, the author notes, are particularly effective against Western leaders because they come (often falsely) within a framework of democratic ideals and upholding the right of people to self-govern.

Undoubtedly, the PRC has studied the information environment in the lead-up to and throughout the 2022 Russian invasion of Ukraine. Chinese strategists are likely formulating narratives to counter the Joseph R. Biden administration's skillful use of intelligence disclosures, such as the proactive "prebuttal" aimed at shaping global opinion against the Russian buildup leading to its invasion of Ukraine in February 2022.[16]

A Better Appreciation for Competition

Combating such nuanced and pervasive information warfare activities requires a greater understanding of the modern competition continuum and how DOD engages our adversaries below the threshold of armed conflict. Such an understanding not only makes clear the PRC's comprehensive, whole-of-government approach to competition, but also reveals the current shortcomings of our bifurcated joint approach to competition that stifles creativity and inhibits combatant commander initiative. Joint Doctrine Note 1-19 (JDN 1-19), *Competition Continuum*, describes competition below armed conflict as nonviolent actions conducted by the joint force or proxies to achieve objectives that are mutually at odds with those of a competitor.[17] Acknowledging that competition requires the whole of government, JDN 1-19 distinguishes between the instruments of national power and those actions reserved specifically for the joint force. At the top, competition consists of "diplomatic and economic activities, political subversion, intelligence and counterintelligence, operations in cyberspace and the information environment, [and] military engagement," while the joint force is left with "security cooperation, military information support, freedom of navigation, and other nonviolent military engagement activities."[18] These separate spheres, and the narrow focus left for the joint force, stand in sharp contrast to the holistic approach espoused by the People's Liberation Army (PLA) and its "Three Warfares" strategy.

Nestled within the PLA's broader strategy of "active defense" is an operational concept uniquely suited for the offense during competition below armed conflict. As the cornerstone of China's global influence operations, the Three Warfares strategy employs psychological warfare, public opinion warfare, and legal warfare to promote a pro-Beijing narrative and set conditions for achieving outcomes favorable to the Chinese Communist Party's strategic objectives.[19] The concept relies on propaganda, deception, threats, and coercion to affect adversary decisionmaking, while propagating targeted narratives and disinformation in public forums to sway key domestic and international audiences.[20] Although its methods are relatively standard, what the Three Warfares concept lacks in ingenuity, it makes up for in scale and scope, effectively bridging the gap between party, state, army, and populace in a distinctly Chinese version of unified action. The United Front Work Department, Propaganda Ministry, State Council Information Office, PLA, and Ministry of State Security are all key actors in a coordinated effort to influence audiences at home and abroad.[21] Acknowledging the breadth and coordination inherent in the Three Warfares concept provides a benchmark for recognizing just how much the joint force must adapt and where it should start if it is to effectively compete with the PRC. Below are four recommendations that will allow the U.S. joint force to prevail in modern warfare.

Recommendation 1: Greater Incorporation of Irregular Warfare & Information Warfare Concepts. To prevail in Great Power competition (GPC), the United States must abandon its myopic view of war and peace as two sharply distinct states in favor of a broader understanding that includes innovative ways and means of operating below the threshold of armed conflict. The foremost way DOD can do this is by redefining irregular warfare to better incorporate information warfare activities to provide the joint force with the tools necessary to operate across the competition continuum.

The current DOD definition of irregular warfare is too narrow to remain relevant in an era defined by GPC. Joint Publication 1 defines *irregular warfare* as "a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s)."[22] Irregular warfare is distinguished from traditional warfare by its non-Westphalian character—its disregard for the norms surrounding state sovereignty and internal affairs. Much like information warfare, irregular warfare approaches are often indirect or asymmetric, tailored to protracted conflicts, and designed to "erode their opponent's power, influence, and will."[23] Both Russia and China practice irregular warfare and information warfare approaches below the level of armed conflict, actively employing their forces to undermine or delegitimize a competitor by controlling the narrative, confusing the situation, and influencing key audiences.

While the overall concept remains viable, the term *violent* in the definition of irregular warfare betrays its intent and is in need of revision. The definitional constraint that describes irregular warfare as a violent struggle limits its conduct to only periods of armed conflict and is a vestige of antiquated U.S. military thinking that embraced a narrow peace-war dichotomy inconsistent with the integrated campaigning model presented in the competition continuum.[24] Campaigning through cooperation, competition, and conflict addresses adversaries who view competition as a constant, uninterrupted struggle for "security, influence, and resources."[25] However, operating along the continuum requires the appropriate tools, and just as "little green men" sowed confusion in Ukraine and "little blue men" made de facto claims to disputed reefs in the South China Sea, the joint force needs creative irregular warfare options it can employ during both competition and conflict.

Although simple, revising the definition of irregular warfare to expand its applicability acknowledges the changing character of warfare reflected in contemporary doctrine, provides greater options for commanders competing below the level of armed conflict, and drives the creativity necessary to prevail in GPC. This is not a call to change policy or authorities but is instead a way of changing how the joint force understands and integrates irregular warfare and information warfare activities in unison below the level of armed conflict. Recent publications such as JDN 1-19 recognize the changing character of warfare and the need to adapt the joint force's approach to competition. Current revisions to Joint Publication 5-0, *Joint Planning*, both highlight the importance of campaigning through competition and emphasize the necessity of multi-domain tactics in 21st-century warfare. Key terms, such as *decisive point*, have been revised to address operations in cyberspace, and likewise, *irregular warfare* should be updated to account for its expanded utility during periods of persistent competition.[26] Other scholars have made similar arguments, pointing to the need for an improved understanding of unconventional warfare (UW)—an irregular warfare mission area—to better compete by disrupting or coercing a competitor.[27] Instead of focusing primarily on support to insurgencies, advocates argue that UW should be plied actively in the information environment, fomenting unrest or coercing adversarial governments. While this change aligns with the position presented here, it is but a part of the cultural shift required to broaden how the joint force understands competition.

Expanding the definition of *irregular* beyond the confines of armed conflict provides combatant commanders with the option of conducting activities usually restricted to a joint operations area or joint special operations area, on an enduring basis, and without the need for national command authority approval, so long as these activities are primarily focused on subverting an adversary's ability to expand its influence within a combatant commander's theater of operations below the level of armed conflict. This expansion aligns with similar discussions surrounding the delegation of authorities for offensive cyber operations that occurred during General Paul Nakasone's Senate confirmation hearing in 2018. In his written testimony, General Nakasone argued that "Based on the evolving nature of adversary cyber capabilities and threats, USCYBERCOM [U.S. Cyber Command] must be postured to defend the Nation in and through cyberspace, which may necessitate conducting certain cyber activities and operations outside of armed conflict or declared areas of hostilities."[28] So too must combatant commanders have the ability to conduct irregular warfare activities below the level of armed conflict; whether through operational preparation of the environment or UW. With this expanded purview, both irregular warfare and information warfare activities can be built into theater campaign plans and will no longer be reserved strictly for contingencies. This will invigorate planning and provide commanders with even more options for campaigning through cooperation, competition, and conflict.

Recommendation 2: Whole-of-Government Approach, Revive the U.S. Information Agency. The U.S. engagement in the information domain cannot be limited to the exclusive capabilities of a single department nor be siloed in its approach. Our adversaries have demonstrated an ability to craft strategic narratives that span the national instruments of power and employ them to great effect. While our current efforts have increased, we cannot expect to compete or dominate until we achieve unity of effort and, ideally, unity of command, in our information campaign. In 1999, years after our victory in the Cold War, we dismantled the U.S. Information Agency (USIA), as there was a perception it was no longer needed. As a result, we lost the ability to marshal the combined effort of our departments under a single Cabinet-level representative who had a "seat at the table" with our nation's leadership.[29] Today, the National Security Council attempts to fill the void of crafting the "position of the Nation" often lacking a unified voice that an established Cabinet-level representative with associated resources would afford. We would implore the Nation's leadership to revisit the idea of a U.S. Information Agency, updated and expanded for the 21st century and the current era of GPC, with the expanded mission of countering foreign malign influence. This cannot be a single department effort or the USIA of the past—the organization must be staffed in an integrated fashion with

Airman 1st Class Cody Moser, left, and Airman 1st Class Calvin Ledford, 18th Communications Squadron expeditionary communications technicians, set up Starlink terminals at Kadena Air Base, Japan, January 10, 2023 (U.S. Air Force/Sebastian Romawac)

those background in the professions of arms, intelligence, law enforcement, and statecraft. DOD would provide members who can assist with crafting and countering strategic narratives and who are knowledgeable about the three stages of narrative creation: formation (how narratives are created), projection (how narratives are spread and contested), and reception (how narratives are received) if we want to "stick the landing."[30] Greater emphasis should be placed on creating an environment where State Department action officers are integrated with a blend of Servicemembers with backgrounds

in foreign area operations (political or regional affairs strategists), information operations, influence operations, public affairs, strategy, intelligence, and cyber warfare. Many who challenge the recreation of a USIA will say that this was an institution designed for a simpler time of bipolarity (United States versus Soviet Union, or "West versus the Rest"), when the world was less digitally connected. With its rebirth, a modern USIA would be charged with marshaling the whole-of-government response to countering foreign disinformation campaigns by consolidating the authorities and capabilities resident in DOD, the Department of Justice, the Department of State, and the Department of Homeland Security under a single organization to operate seamlessly to counter foreign disinformation threats to the United States.

Recommendation 3: Building and Retaining a National Cyber Force. In 1933, Franklin D. Roosevelt enacted the New Deal, consisting of a series of workforce programs designed to not only revitalize the Nation's workforce but also restore the competitive advantage of the United States. A key aspect of the New Deal centered on an initiative called the Civilian Conservation Corps (CCC), a program focused on recruiting, training, employing, and ultimately reinvigorating a young cadre of Americans whose sole focus would be to rebuild, restore, and preserve the Nation's critical infrastructure, Federal lands, and natural resources during a time of domestic turmoil and global uncertainly.

Today, the Nation is at an inflection point whereby Americans' science, math, engineering, and digital literacy is eroding at an alarming rate compared with that of our PRC competitor. And despite billions of dollars' worth of investments in the information technology and security programs, DOD is unable to generate the capacity required to cover in totality the scope and scale of espionage and cyber attacks posed by our Great Power adversaries.

Much like the CCC in 1933, DOD could take the lead in revisiting what service to the Nation looks like (beyond today's traditional uniformed armed Services) in the 21st-century information age, especially in technical fields of computer engineering, information technology, and cyber security. In that scenario, the Nation would be formulating the means to harness the voluntary energy of technically gifted patriotic American citizens at a young age, with minimal investment. Much as the CCC of the past provided the core of the U.S Army's noncommissioned officer corps during World War II, an information-centric version of the CCC would offer a means for our nation's technically gifted to serve in a reserve "Civilian Cyber Corps" and to be called on to augment the defense of critical infrastructure sectors in a time of national crisis. Recent events have shown that neither DOD nor the U.S. Government has the capacity or skill sets to effectively secure our nation's cyberspace and critical infrastructure sectors from cyber attacks. The establishment of a Civilian Cyber Corps would be a worthy investment, enabling the Nation to rapidly cultivate young technical talent while simultaneously providing an avenue for service to the country.

Taking a note from history, a Civilian Cyber Corps would be centered on establishing a framework whereby our nation's technical talent could be cultivated at an early age and offered streamlined pathways to serve their nation outside of a traditional military uniformed Service framework. A Civilian Cyber Corps would bolster the means to support the DOD's Defense Support to Civil Authorities mission with leadership predominantly coming from the Reserves or National Guard due to the components' strong ties to industry, along with partnerships to establish the connective tissue necessary to defend and secure the Nation at the state and Federal levels. It would offer not only technical training but also employment, from basic information systems administration to something as advanced as malware analysis and threat heuristics.

Structurally, the Civilian Cyber Corps would be focused on three broad lines of effort, consisting of recruitment, development, and integration into existing Federal and state cyber security organizations. From a recruitment and development standpoint, the Civilian Cyber Corps would focus on developing digital literacy and cultivating technical talent along a broad spectrum of sectors, from grade school youths all the way to young adults under 25 years old. Much like the Boy Scouts of America, participants of the program would be incentivized by technical training opportunities, Federal grants, academic scholarships, and even streamlined appointments to participating U.S. military academies and participating universities later on, if participants demonstrated continued interest and dedication. Upon graduation, participants would be offered internships in technology companies, government sectors, and, if they should so choose, appointments to the Armed Forces Reserves, designed to be called on in times of national emergency such as a cyber attack on critical infrastructure or to support key national-level cyber initiatives. From an integration standpoint, the Civilian Cyber Corps would offer maximum capacity to serve across Federal, state, and local governments, and potentially private-sector organizations. A modern Civilian Cyber Corps would create a "digital bench" for our Federal and state leaders to recruit and draw from as a means to resource and even lead the multitude of cyberspace and information technology across the national security apparatus. Now more than ever, the Nation needs bold ideas and creative methods to cultivate, recruit, and ultimately employ the full extent of its technical prowess to address 21st-century information age challenges. The establishment of a Civilian Cyber Corps would revolutionize service to the Nation in the 21st century while sparking the competitive spirit of young Americans outside of traditional military service that is needed to win against our nation's Great Power adversaries.

Finally, the establishment of a Civilian Cyber Corps would help DOD formulate the precursor and establishment of a seventh military branch—U.S. Cyber Force—a Service dedicated solely to organizing, training, and equipping offensive and defensive cyber forces to defend the Nation, secure its networks, and support its traditional military activities. The Civilian Cyber Corps could be a natural feeder into this new military Service, one that starts the recruitment and development of digital talent at a young age for service to the Nation. Also, a Civilian Cyber Corps would provide a natural Reserve Component for those who seek respite from Active duty and would like to seek opportunities outside the military while still serving in a limited capacity. It is time for DOD to recognize that since the establishment of the Cyber Mission Forces (USCYBERCOM's action arm), the force's readiness, capacity, and retention have steadily declined while the requirements placed on these low-density and high-demand forces continue to increase. The way each military Service organizes, trains, and equips our cyber forces is currently disjointed, cumbersome, overly bureaucratic, and ultimately lacks institutional support for greater resourcing, since cyber operations is not each of the Services' primary mission. Countless congressional hearings centered on the retention of cyber professionals have proved that the mechanisms we have in place—whether they are cyber-excepted service for civilians or direct commissioning mechanisms into the Armed Services—have proved to be both insufficient and unable to scale to meet the demands placed on the force. Much as there is a need to establish an organization dedicated to recruitment and development of digital talent at a young age by way of a Civilian Cyber Corps, so is there a need for the U.S. military to have a separate and distinct Service dedicated to the organization, training, and equipping of cyber warfare forces if we want to build a force that is postured to fight and win in the information environment.

Conclusion

In the face of unprecedented challenges and threats to our democracy, we must be prepared to take bold actions at this critical juncture in our nation's history. The recent convergence of Russian and Chinese actions in the information space proves that the risk of inaction is far too great. Initiative loss in this arena is rarely recoverable, and its impact will span generations of Americans and democratic nations around the world now and into the future. The competition continuum is vast and complex, and it extends far beyond DOD's authorities alone.

The time for courageous new approaches is now. We must implement swift changes to antiquated ideologies that handcuff the joint force's ability to maneuver in this dynamic battlespace. Therefore, we believe DOD must expand its definition of irregular warfare to reflect a modern competition continuum, advocate with our interagency partners to build a central U.S. information agency, and finally, establish a new framework for service to the Nation outside the traditional uniformed Services. This would be accomplished through the establishment of a Civilian Cyber Corps, which would leverage our nation's digital talent for the national defense and would act as a means to build a future United States Cyber Force. Together, these reforms will enable the joint force to maintain its competitive edge over our adversaries today and protect the values at the heart of our nation's democracy in the future. **JFQ**

Notes

[1] Basil Henry Liddell Hart, *Strategy*, 2nd ed. (New York: Signet, 1974), 5.

[2] Conor Cunningham, "A Russian Federation Information Warfare Primer," The Henry M. Jackson School of International Studies, November 12, 2020, available at <https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/>.

[3] Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no. 2 (2004), 237–256.

[4] Brenna Cole and George Noel, "Nation-State Perspectives on Information Operations and the Impact on Relative Advantage," paper presented at the International Conference on Cyber Warfare and Security, February 2021.

[5] Dave Johnson, "ZAPAD 2017 and Euro-Atlantic Security," *NATO Review*, December 14, 2017, available at <https://www.nato.int/docu/review/articles/2017/12/14/zapad-2017-and-euro-atlantic-security/index.html>.

[6] Andreas Ventsel et al., "Discourse of Fear in Strategic Narratives: The Case of Russia's Zapad War Games," *Media, War & Conflict* 14, no. 1 (March 2021), 24–26.

[7] Sheena Chestnut Greitens, Myunghee Lee, and Emir Yazici, "Understanding China's 'Preventive Repression' in Xinjiang," *Order From Chaos* (blog), March 4, 2020, available at <https://www.brookings.edu/blog/order-from-chaos/2020/03/04/understanding-chinas-preventive-repression-in-xinjiang/>.

[8] "Hong Kong Security Law: Anger as China's XI Signs Legislation," BBC, June 30, 2020, available at <https://www.bbc.com/news/world-asia-china-53234255>.

[9] Tom O'Connor, "China Hosts Russia Troops to Hold Strategic Military Drills for First Time," *Newsweek*, August 2, 2021, available at <https://www.newsweek.com/china-hosts-russia-troops-hold-strategic-military-drills-first-time-1615496>.

[10] Elizabeth Chen, "China Learning From Russia's 'Emerging Great Power' Global Media Tactics," *China Brief* 21, no. 7 (April 12, 2021), available at <https://jamestown.org/program/china-learning-from-russias-emerging-great-power-global-media-tactics/>.

[11] Ibid.

[12] Kristin Huang, "Can Beijing Use Lessons Learned by Europe to Ease South China Sea Tensions?" *South China Morning Post*, November 9, 2019, available at <https://www.scmp.com/news/china/diplomacy/article/3036788/can-beijing-use-lessons-learned-europe-ease-south-china-sea>.

[13] Chen, "China Learning From Russia's 'Emerging Great Power' Global Media Tactics."

[14] Gary Rawnsley, "To Know Us Is to Love Us: Public Diplomacy and International Broadcasting in Contemporary Russia and China," *Politics* 35, nos. 3–4 (2015), 273–286, available at <https://doi.org/10.1111/1467-9256.12104>.

[15] *China's Military Power: Modernizing a Force to Fight and Win* (Washington, DC: Defense Intelligence Agency, 2019), 4–140.

[16] Jake Harrington, "Intelligence Disclosures in the Ukraine Crisis and Beyond," *War on the Rocks*, March 1, 2022, available at <https://warontherocks.com/2022/03/intelligence-disclosures-in-the-ukraine-crisis-and-beyond/>.

[17] Joint Doctrine Note (JDN) 1-19, *Competition Continuum* (Washington, DC: The Joint Staff, June 3, 2019), 4–7, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf>.

[18] Ibid., 2.

[19] *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020* (Washington, DC: Office of the Secretary of Defense, 2020), 130, available at <https://media.defense.gov/2020/sep/01/2002488689/-1/-1/1/2020-dod-china-military-power-report-final.pdf>.

[20] Ibid.

[21] Ibid.

[22] Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013, Incorporating Change 1, July 12, 2017), I-6, available at <https://irp.fas.org/doddir/dod/jp1.pdf>.

[23] Ibid.

[24] JDN 1-19, *Competition Continuum*, 4–7.

[25] Blagovest Tashev, Michael Purcell, and Brian McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," *MCU Journal* 10, no. 2 (2019), 141, available at <https://dx.doi.org/10.21140/mcuj.2019100208>.

[26] JP 5-0, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), IV-32, available at <https://irp.fas.org/doddir/dod/jp5_0.pdf>.

[27] Otto C. Fiala and Jim Worrall, "Imposing Costs: Unconventional Warfare in the Information Environment," *Modern War Institute*, July 6, 2021, available at <https://mwi.usma.edu/imposing-costs-unconventional-warfare-in-the-information-environment/>.

[28] Senate Armed Services Committee, Advance Policy Questions for Lieutenant General Paul Nakasone, USA, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, 115th Cong., 2nd sess., 2018, 31, available at <https://www.armed-services.senate.gov/imo/media/doc/Nakasone_APQs_03-01-18.pdf>.

[29] Dr. Vivian Walker, email, July 22, 2021, following author's presentation, "Countering Disinformation Narratives: Strategic Approaches," Joint Combined Warfighting School, Norfolk, VA, July 16, 2021.

[30] Alister Miskimmon, Ben O'Loughlin, and Laura Roselle, *Forging the World: Strategic Narratives and International Relations* (Ann Arbor: University of Michigan Press, 2017).